GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad 27 July, 2021

28 JUL 2021

M(Admin/HR)

Subject: **Cyber Security Advisory - Email Containing Malicious Attachment File (Advisory No. 48)**

A.S (Rev. Div.)

M(I.T)

1. An advanced malware has been identified which is spreading through an email with the subject **"Matrimonial_biodata"** among defence and civil organizations for information gathering and system control. This spoofed email has executable **.zip** file that contains **.exe** and **.docx** files to infect targeted systems. On clicking these files, a photo is opened that runs a malware in background. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned and adopt recommended preventive measures.

2. Forwarded for information and dissemination to all concerned, please.

Major
(Imran Nazir)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Secretary, NTISB, Cabinet Division, Islamabad
7. Deputy Secretary, NTISB, Cabinet Division, Islamabad
8. Director (IT), Cabinet Division, Islamabad

CIO [illegible] I.T

[illegible] 29/7

(IT-II)

Annex-A

Cyber Security Advisory - Email Containing Malicious Attachment File (Advisory No. 48)

1. Recently, a targeted malware is spreading through email with the subject **"Matrimonial_biodata"** among defence and civil organizations for information gathering and system control. This spoofed email has executable **.zip** file that contains **.exe** and **.docx** files to infect targeted systems. On clicking these files; a photo is opened that runs a malware in background. The email is a sophisticated targeted phishing attack, therefore, recommended measures at Para 4 must be adopted.

2. **Summary of Malicious Email**

a. **File Name.** Matrimonial_biodata.zip

b. **Files included**

Ser	Files
(1)	Tani_Khan_Matrimonial_biodata_for_email_circulation.doc
(2)	Tani_Khan_MatrimonialLbiodata_for_email_circulation.exe
(3)	Tani_Khan_Matrimonial_biodata_for_email_circulation_2.exe
(4)	Tani_Khan_Matrimonial_biodatajor_for_email_circulation_3.exe
(5)	Tani_Khan_MatriMonial_biodata_for_email_circulation_4.exe

c. The malicious files are dropped at following system locations to gain persistence: -

(1) C:/Users/<user>/Appdata/Roaming/Microsoft/Windows/Update/**Rasdial.exe**

(2) C:/Users/<user>/Appdata/Roaming/Microsoft/**MicroScMgmt.exe.**

(3) **Persistence as Startup** set to **dwme.lnk** with value C:/Users/<user>/Appdata/Roaming/Microsoft/Windows/Update/**Rasdial.exe**

(4) **Persistence as Task scheduler** set to **/TestDailyTrigger** with value C:/Users/<user>/Appdata/Roaming/Microsoft/**MicroScMgmt.exe.**

d. **C&C Servers**

Ser	IP Address	Country
(1)	142.202.191.234	US (Whitelisted IPs)
(2)	142.202.191.236	

3. **Capabilities of Malware**

a. The **macro** based malware is specially designed for targeted attacks and can steal files / saved passwords from Windows system and browsers.

b. The malware is a **file stealer** built on another malware **HomeTelem.exe.**

c. The attack involves **Windows certificates alterations** to reside for persistence at **multiple locations.**

d. The malware employs sleep function as **defensive technique;** makes multiple copies of scripts are made for **persistence** and checks for **presence of debugger:**

e. The malware contains images laced with executables that run as **verified** legitimate and **verified files.**

f. The attacker can gain **remote access of the system** and can execute additional payload.

4. **Recommendations**. Above in view, following is recommended: -

a. Block IPs on Firewall / IDS system / Email server which are mentioned in para (**2 (2d)** to ensure malware communication is halted.

b. Disable **macros** to ensure malware files of similar nature do not get executed.

c. Administrators to **limit priviledges** of users by **Group Policies on domain** or **Firewall** to avoid running **.exe files** that will stop malware execution.

d. **Disable Microsoft Equation Editor in MS-Office** from **registry** to avoid further attacks.

e. **Do not download attachments from emails unless you are sure about the source.**

f. Window defender and Firewall of system to be kept on recommended settings.

g. Be vigilant regarding redirected links and typing censive information online.

5. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

6. Forwarded for perusal and dissemination of information to all concerned and under command, please.